ASD(C3I)
..614-1802

June 26, 1981
NUMBER 4640.6

(2)

USD(P)

Department of Defense Directive

SUBJECT: Communications Security Telephone Monitoring and Recording

References: (a) DoD Directive 4640.1, "Telephone Monitoring and Recording," January 15, 1980
(b) through (p), see enclosure 1

A. PURPOSE

This Directive establishes policy and procedures for the communications security (COMSEC) monitoring and recording of telephone communications.

B. APPLICABILITY

1. This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies (hereafter referred to as "DoD Components").

2. This Directive does not apply to signals intelligence; administrative telephone monitoring and recording (reference (a)); interception of oral and wire communications for law enforcement purposes (DoD Directive 5200.24 (reference (b)); technical surveillance countermeasure surveys (DoD Directive 5200.29 (reference (c)); control of compromising emanations (DoD Directive S-5200.19 (reference (d)); management and direction of COMSEC activities (DoD Directive C-5200.5 (reference (e)); foreign intelligence and counterintelligence activities (DoD 5240.1-R (reference (f)); Foreign Intelligence Surveillance Act of 1978 (reference (g)); and telephone monitoring during wartime or under combat conditions (DoD Directive 5230.7 (reference (h)).

C. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

D. POLICY

1. COMSEC telephone monitoring is a valuable asset of the U.S. Government which must be conducted in a manner that satisfies the legitimate needs of the government and protects the privacy and civil liberties of persons whose telephone communications are subject to such monitoring.

2. DoD-owned or leased telephones and telephone systems are provided for the transmission of official government communications and are subject to COMSEC telephone monitoring in accordance with this Directive, the National Communications Security Directive (reference (i)) and National COMSEC Instruction 4000 (reference (j)). Use of official DoD telephones and telephone systems constitutes consent by the user to COMSEC telepone monitoring.

3. COMSEC telephone monitoring provides information not available through other sources that is essential for evaluation of DoD communications security.

4. COMSEC telephone monitoring is undertaken to:

a. Collect operational signals to measure the degree of security achieved by U.S. codes, cryptographic equipment and devices, COMSEC techniques, and related measures;

b. Determine the information and intelligence value of voice communications potentially subject to interception;

c. Provide an empirical basis for improving, as effectively and efficiently as possible, the security of telephone communications against hostile interception; and

d. Assist in developing communications profiles for cover and deception measures.

5. COMSEC telephone monitoring within the Department of Defense shall be conducted only by elements of the National Security Agency/Central Security Service (NSA/CSS) and the Military Departments specifically and as designated by the Director of NSA/Chief, CSS, and the Secretaries of the Military Departments, respectively.

E. PROHIBITIONS

1. This Directive does not authorize electronic surveillance of telephone communications for law enforcement or investigative purposes, and, except as provided in this section, the information obtained from COMSEC telephone monitoring shall not be used for law enforcement or investigative purposes.

2. The sole exception to this policy is when, incidental to the COMSEC telephone monitoring authorized by this Directive, information is obtained which requires immediate action in order to prevent serious bodily harm or significant loss of property. Such information may be referred to the commander or law enforcement agency having jurisdiction over the incident. In such instances:

a. The General Counsel of the DoD Component involved shall be notified promptly.

b. COMSEC telephone monitoring of the telephone circuit concerned shall cease. No attempt to investigate further or to obtain specifically additional information of criminal activity through COMSEC telephone monitoring will occur. Any subsequent electronic surveillance shall be conducted in accordance with DoD Directive 5200.24 (reference (b)) or DoD 5240.1-R (reference (f)), as appropriate.

3. This prohibition does not preclude the use of information obtained as a result of COMSEC telephone monitoring in connection with disciplinary or administrative action against DoD military or civilian personnel for knowing, willful, or negligent actions that resulted in the unauthorized disclosure of classified information.

4. COMSEC telephone monitoring or the results of COMSEC telephone monitoring shall not be used to enforce the DoD policy that limits use of DoD telephones and telephone systems to conduct of official business only. That policy shall be enforced through administrative and management techniques, such as, analysis of system-wide records, periodic briefings, and supervisory controls.

F. PROCEDURES

The procedures in this section apply to all COMSEC telephone monitoring of official DoD telephones in DoD Components.

1. Notice and Consent. Users of official DoD telephones and telephone systems shall be notified that discussion of classified information over nonsecure circuits is prohibited, official DoD telephones and telephone systems are subject to COMSEC telephone monitoring at all times, and use of such telephones and telephone systems constitutes consent to COMSEC telephone monitoring.

a. The following notice shall be displayed prominently on the cover of all official DoD telephone directories:

> DO NOT DISCUSS CLASSIFIED INFORMATION ON NONSECURE TELEPHONES. OFFICIAL DOD TELEPHONES ARE SUBJECT TO MONITORING FOR COMMUNICATIONS SECURITY PURPOSES AT ALL TIMES.
>
> DoD telephones are provided for the transmission of official government information only and are subject to communications security monitoring at all times. Use of official DoD telephones constitutes consent to communications security telephone monitoring in accordance with DoD Directive 4640.6.

b. In addition to the telephone directory notice, all Heads of DoD Components shall ensure that users of official DoD telephones and telephone systems subject to COMSEC telephone monitoring receive adequate notice that their use of such telephones and telephone systems constitutes consent to COMSEC telephone monitoring. Such other forms may include, but need not be limited to, the following:

(1) Decals (DD Form 2056) attached to telephones subject to COMSEC telephone monitoring. See enclosure 3;

(2) A notification and consent form;

(3) Special memoranda from responsible senior officials;

(4) Initial briefing of new personnel and periodic rebriefings;

(5) Periodic notices in daily bulletins and similar publications; and

(6) Other means approved by the General Counsel of the DoD Component concerned.

c. The General Counsel of each DoD Component shall review the notification given to users of the Component's official DoD telephones and telephone systems subject to COMSEC telephone monitoring at least once every 2 years, and shall state in writing his or her determination of the adequacy or inadequacy of such notification to include the reasons supporting that determination. If notification is inadequate, he or she shall require implementation of those measures necessary to make notification adequate.

2. Authorization and Request

a. COMSEC telephone monitoring may be authorized only by the Secretaries of the Military Departments, the Director, NSA/Chief, CSS, and Commanders of Unified or Specified Commands, or their single designees. COMSEC telephone monitoring shall be authorized only:

(1) In DoD Components in which the Component's General Counsel has determined, pursuant to paragraph F.1.c. of this Directive, that adequate notification exists;

(2) When it will aid in protecting the national security;

(3) When it will be an effective and efficient use of COMSEC resources. This determination shall be made in consultation with the operational COMSEC elements designated pursuant to paragraph F.3.a., below; and

(4) For a reasonable period of time not to exceed 1 year.

b. Heads of DoD Components other than the Military Departments, Unified and Specified Commands, and NSA/CSS shall submit requests for COMSEC telephone monitoring to the Director, NSA/Chief, CSS, in accordance with regulations of the NSA/CSS.

c. COMSEC telephone monitoring within OSD and the Defense Telephone Service-Washington is prohibited except with the written approval of the Deputy Under Secretary of Defense for Policy, or a designee.

3. Monitoring Procedures

a. COMSEC telephone monitoring within the Department of Defense shall be conducted only by elements of NSA/CSS and the Military Departments, specifically designated respectively by the Director of NSA/CSS and the Secretaries of the Military Departments.

b. COMSEC telephone monitoring of telephone lines within the Department of Defense shall be conducted only from points within the facilities or installations of DoD Components by bridging the telephone lines at points prior to the point of association, in a main distribution frame, between official DoD telephones lines and outside lines.

c. COMSEC telephone monitoring of radio, microwave, and other free space official telephone communications shall not be conducted, except for those official telephone communications that are transmitted over systems dedicated solely to government use and that are sent and received by transmission and reception facilities dedicated solely to government use.

4. Acquisition, Retention, and Storage Procedures. The following procedures apply to the acquisition, retention, and storage of information respecting telephone conversations acquired in the course of COMSEC telephone monitoring or produced in the course of analyzing such information.

a. COMSEC telephone monitoring shall be conducted in a manner that minimizes, to the fullest extent possible, consistent with operational requirements, the recording of communications not relevant to the COMSEC telephone monitoring mission.

b. If practical, information extraneous to the COMSEC telephone monitoring mission shall be expunged from recordings upon recognition. Any such information present on recordings, to include the identities of individual conversants, will not be transcribed or otherwise used unless required in support of actions identified in subsections E.2. and E.3.

c. All transcripts, notes, logs, and other written working materials produced in the course of COMSEC telephone monitoring or in the course of analyzing communications acquired through COMSEC telephone monitoring shall be reviewed within a reasonable period after the production of such written material to assure that information not relevant of COMSEC purposes inadvertently included has been expunged. Material retained shall be annotated to include the name of the person who conducted the review and the date of the review.

d. Except as provided below, all recordings, transcripts, notes, logs, and any other written working materials containing information acquired in connection with COMSEC telephone monitoring shall be erased or destroyed upon the issuance of a final report based upon those records or within 1 year, whichever is earlier.

e. Recordings and written working materials may be retained beyond 1 year of the issuance of a final report, only if such retention is necessary for the COMSEC mission and is first approved by officials designated by the Director, NSA/Chief, CSS, for that Agency, or by the Secretaries of the Military Departments for their respective Departments.

(1) Prior to approving extended retention, the approving officials shall determine whether the material to be retained has been adequately reviewed for identification and expunction of all information not relevant to COMSEC purposes. The officials shall provide for additional review of the material, if not satisfied that adequate review has occurred.

(2) Approval of extended retention shall be in writing and shall stipulate the period of time for which the recordings or written working materials may be retained.

(3) Upon the expiration of the extended retention period, the recordings or written materials shall be erased or destroyed. No information shall be retained in any form, including recordings, written working materials, or computerized data banks, after the extended retention period has expired.

(4) This paragraph does not apply to final reports resulting from a COMSEC telephone monitoring operation.

f. Final reports or evaluations resulting from a COMSEC telephone monitoring operation:

(1) Will be retained in accordance with established record retention procedures;

(2) Shall not contain:

(a) Any information extraneous to COMSEC purposes;

(b) Accounts or summaries of particular telephone conversations monitored, except for descriptions of information that may be classified or national security-related discussed in such conversations and information necessary to understand the nature of and ways in which classified information may have been compromised; or

(c) Sufficient data to identify individuals who participated in monitored telephone conversations.

(3) Shall have an access clause prominently displayed at the beginning of the report stating that the information in the report shall be used only for official U.S. Government COMSEC purposes.

g. To the extent consistent with E.O. 12065 and DoD 5200.1-R (references (k) and (l)), all recordings and written working material containing information acquired through COMSEC telephone monitoring shall be afforded protection at least equal to that provided material officially classified CONFIDENTIAL.

h. Except as provided in subsection F.5. of this Directive, access to any recordings, written working materials, or computerized data banks containing information acquired through COMSEC telephone monitoring shall be limited to individuals in the DoD Components designated, pursuant to F.3.a. of this Directive and assigned to COMSEC duties requiring such access. Recordings, written working materials, and computerized data banks shall be stored and maintained in a manner that will assure enforcement of these access restrictions.

5. Dissemination Procedures

a. Information respecting telephone conversations acquired through COMSEC telephone monitoring shall be disseminated outside the Department of Defense only in the following circumstances:

(1) For purposes permitted by subsections E.1. through E.3. of this Directive;

(2) Pursuant to the provisions of DoD 5200.1-R (reference (l)); and

(3) When required by a court order and approved by the General Counsel of the Department of Defense.

b. Information acquired by COMSEC telephone monitoring under this Directive shall be disseminated within or outside of the Department of Defense only as necessary for purposes of COMSEC operation and management or as provided for in subsections E.1. through E. 3. of this Directive. No information shall be disseminated within or outside of the Department or outside the operational COMSEC elements designated pursuant to paragraph F.3.a. of this Directive, unless the reviews required by paragraphs F.4.b. and c. of this Directive have been conducted.

6. Safeguarding Monitoring Equipment. Telephone monitoring and recording equipment shall be safeguarded to prevent unauthorized access.

a. To the extent consistent with operational requirements, equipment not in use shall be kept in secure and controlled storage.

b. Each element of the Military Departments and NSA/CSS authorized to conduct COMSEC telephone monitoring under paragraph F.3.a. of this Directive shall maintain records showing its inventory of COMSEC telephone monitoring equipment, the time at which each item of equipment was withdrawn from and returned to storage, the location and use of each item of equipment currently in use, and the person or persons in charge of the operation for which the equipment is being used.

c. Only those persons assigned to COMSEC duties with an element designated pursuant to paragraph F.3.a. of this Directive, shall have access to monitoring equipment in use.

7. COMSEC Telephone Monitoring Outside DoD

a. COMSEC telephone monitoring by DoD personnel of official government telephone communications outside the Department of Defense is prohibited except upon written authorization of the:

(1) Deputy Under Secretary of Defense for Policy, whenever the COMSEC telephone monitoring is to be conducted by an element of one of the Military Departments.

(2) Director, NSA/Chief, CSS, whenever the COMSEC telephone monitoring is to be conducted by that Agency.

b. Only the elements of NSA/CSS and the Military Departments specifically designated to conduct COMSEC telephone monitoring within the Department of Defense shall conduct COMSEC telephone monitoring outside the Department.

c. COMSEC telephone monitoring operations outside the Department of Defense shall be subject to restrictions respecting notice to telephone users, acquisition, retention, and dissemination of information and safeguarding of monitoring equipment equivalent to the restrictions imposed by this Directive upon such activities within the Department of Defense.

G. INFORMATION REQUIREMENTS AND RESPONSIBILITIES

1. The Deputy Under Secretary of Defense for Policy or designee shall review and provide overall policy guidance for the COMSEC telephone monitoring program and review and act upon requests for COMSEC telephone monitoring in accordance with paragraphs F.2.c. and F.7.a.(1) of this Directive.

2. The Director, NSA/Chief, CSS, and the Secretaries of the Military Departments shall supervise and issue directives to govern all COMSEC telephone operations and ensure that all such operations comply with this Directive. The Director and Secretaries shall each designate one official in their respective Agency or Department as the official with responsibility for oversight of COMSEC telephone monitoring to ensure compliance with the provisions of this Directive.

3. The Head of each DoD Component shall:

a. Authorize or request COMSEC telephone monitoring in accordance with the provisions of this Directive and relevant regulations of the Military Departments and NSA/CSS; and

b. Cooperate with the Director, NSA/Chief, CSS, the Secretaries of the Military Departments, the General Counsels of the DoD Components, and their designees, to ensure that the COMSEC telephone monitoring conducted within the Components is effective and complies with this Directive.

4. All records of information obtained through COMSEC telephone monitoring and associated analysis shall be maintained and disseminated in accordance with subsections F.4. and F.5. of this Directive and with the provisions of DoD Directives 5400.7 and 5400.11 (references (m) and (n)).

5. DoD Components shall report to the Deputy Under Secretary of Defense for Policy, through the General Counsels and Inspector Generals of the monitoring Component and the Component being monitored, within 5 days after discovery all telephone monitoring and recording activities conducted in violation of the provisions of this Directive.

a. These reports shall contain, at a minimum, the following items:

(1) Nature of the violation, such as, unauthorized COMSEC monitoring:

*(2) Date of violation occurrence;

(3) Time of violation occurrence;

*(4) Location (name of installation/activity) where the violation occurred;

*(5) Individual (last name, first, M.I.) or Component responsible for the infraction;

(6) Brief summary of the incident;

(7) Corrective action taken; and

(8) Current status of the inquiry.

b. This reporting requirement has been assigned *Report Control Symbol* DD-POL(AR) 1564. Existing standard data elements from DoD 5000.12-M (reference (o)) are being used in this reporting requirement. Any new data elements will be registered with the Director for Management Information Control and Analysis, Office of the Assistant Secretary of Defense (Comptroller). Data elements marked with an asterisk have been registered in the DoD Data Element Program.

c. Upon receipt of these reports, the Deputy Under Secretary of Defense for Policy and the Inspector Generals and General Counsels of the DoD Components involved shall work together to ensure that all appropriate action is taken to correct and prevent such violations.

H. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward two copies of implementing documents to the Deputy Under Secretary of Defense for Policy within 120 days.

Frank C. Carlucci
Deputy Secretary of Defense

Enclosures - 3
1. References
2. Definitions
3. Decal

REFERENCES, continued

(b) DoD Directive 5200.24, "Interception of Wire and Oral Communications for Law Enforcement Purposes," April 3, 1978
(c) DoD Directive 5200.29, "DoD Technical Surveillance Countermeasures (TSCM) Survey Program," February 12, 1975
(d) DoD Directive S-5200.19, "Control of Compromising Emanations," February 10, 1968
(e) DoD Directive C-5200.5, "Communications Security (COMSEC)," April 13, 1971
(f) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," November 1979, authorized by DoD Directive 5240.1, November 30, 1979
(g) Foreign Intelligence Surveillance Act of 1978, Public Law No. 95-511
(h) DoD Directive 5230.7, "Wartime Information Security Program (WISP)," June 25, 1965
(i) National Communications Security Directive, June 20, 1979
(j) National COMSEC Instruction (NACSI) 4000, "Guidelines for the Conduct of Communications Security Survey Activities," January 23, 1980
(k) Executive Order 12065, "National Security Information," July 3, 1978
(l) DoD 5200.1-R, "Information Security Program Regulation," October 1980, authorized by DoD Directive 5200.1, November 29, 1978
(m) DoD Directive 5400.7, "DoD Freedom of Information Act Program," March 24, 1980
(n) DoD Directive 5400.11, "Personal Privacy and Rights of Individuals Regarding Their Personal Records," August 4, 1975
(o) DoD 5000.12-M, "DoD Manual for Standard Data Elements," June 30, 1980, authorized by DoD Instruction 5000.12, April 27, 1965
(p) DoD Directive 5160.9, "Defense Telephone Service-Washington (DTS-W)," March 22, 1973

DEFINITIONS

1. Communications Security (COMSEC). Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, emissions security, and jamming resistance) to telecommunications and to electrical systems generating, handling, processing, or using national security or national security-related information. It also includes the application of physical security measures to COMSEC information or materials.

2. COMSEC Surveillance. The systematic examination of telecommunications to determine the adequacy of COMSEC measures, to identify COMSEC deficiencies, to provide data from which to predict the effectiveness of proposed COMSEC measures, and to confirm the adequacy of such measures after implementation.

3. COMSEC Telephone Monitoring. Listening to, copying, or recording by any means the content of official telephone communications to provide material for analysis to determine the degree of security being provided to those communications. COMSEC telephone monitoring is one of the techniques of COMSEC surveillance.

4. Consent. The agreement by a person to permit DoD communications security components to monitor the person's official telephone communications. Consent may be oral, written, or implied. Consent may be implied if adequate notice is provided that use of official government telephones carries with it the presumption of consent.

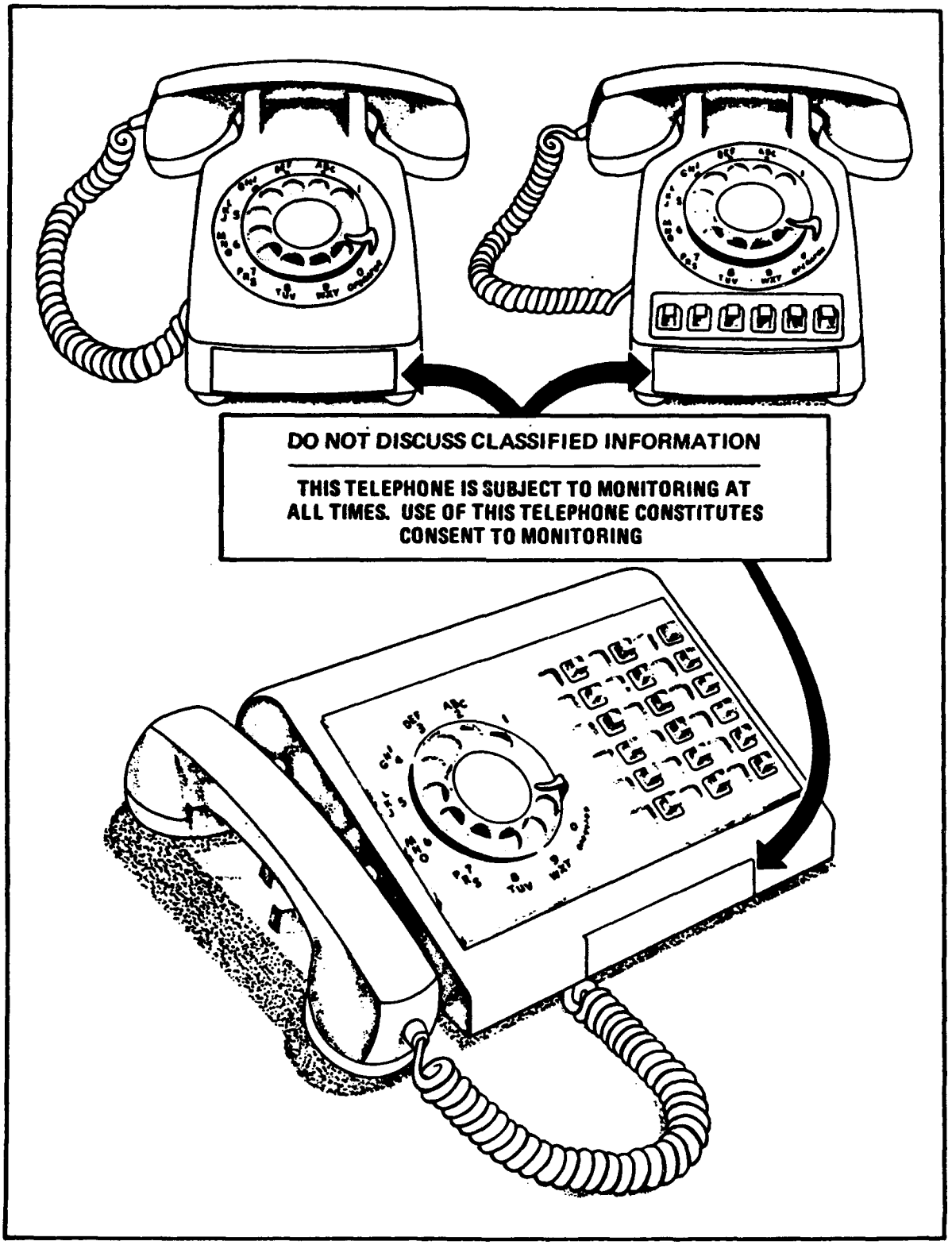
5. Defense Telephone Service-Washington (DTS-W). An organizational entity under the Secretary of the Army that has been assigned responsibility pursuant to DoD Directive 5160.9 (reference (p)) to provide administrative telephone communications, including AUTOVON services, to DoD elements located in the National Capital Region (NCR). The NCR includes the District of Columbia, Montgomery and Prince George's Counties in Maryland, Arlington, Fairfax, Loudoun, and Prince William Counties in Virginia, and the cities of Alexandria, Fairfax, and Falls Church in Virginia.

6. Main Distribution Frame. A distribution frame, on one part of which terminates the permanent outside lines entering the central telephone and communication facility and on the other part of which terminates the subscriber line multiple cabling. The main distribution frame is used for associating any outside line with any desired terminal in such a multiple or with any other outside lines.

7. Official DoD Telephones and Telephone Systems. Telephones or telephone systems owned or leased by the U.S. Government and used for official business purposes of the U.S. Government, including the purposes of command and control of the armed forces. Official DoD telephones do not include pay telephones, telephones that are routinely used by the press, and telephones that are located in individual or family residences and intended for private use, even when the U.S. Government owns such residences.

8. Official Telephone Communications. Telephone communications in which one or more of the parties to the communications uses an official DoD telephone.

DECAL


DO NOT DISCUSS CLASSIFIED INFORMATION
THIS TELEPHONE IS SUBJECT TO MONITORING AT ALL TIMES. USE OF THIS TELEPHONE CONSTITUTES CONSENT TO MONITORING